

CLAIMS

What is claimed is:

- 1 1. A smart card comprising:
2 an interface with a smart card reader;
3 first circuitry configured to receive a first enable signal from a smart card
4 enabler; and
5 second circuitry coupled with the interface and first circuitry and
6 configured to allow the smart card to function with the smart card reader based
7 on the first enable signal.
- 1 2. The smart card of claim 1, wherein the first circuitry is also configured to
2 receive a second enable signal from the smart card enabler, and wherein the
3 second circuitry is also configured to allow the smart card to perform a
4 transaction with the smart card reader based on the second enable signal.
- 1 3. The smart card of claim 2, wherein the first enable signal and the second
2 enable signal are radio frequency signals.
- 1 4. The smart card of claim 2, wherein the second circuitry is also configured
2 to disable the smart card to function with the smart card reader if the first
3 circuitry does not receive the first enable signal.
- 1 5. The smart card of claim 2, wherein the second circuitry is also configured
2 to disable the smart card to perform the transaction with the smart card reader
3 if the first circuitry does not receive the second enable signal.

1 6. The smart card of claim 2, wherein the second circuitry is also configured
2 to disable the smart card to perform the transaction after a predetermined time
3 period.

1 7. The smart card of claim 2, wherein the second circuitry performs the
2 transaction with the smart card reader through the interface after receiving the
3 first enable signal and the second enable signal.

1 8. The smart card of claim 7, wherein the second circuitry performs the
2 transaction for the smart card that is within a close proximity of the smart card
3 enabler.

1 9. The smart card of claim 1, wherein the second circuitry includes:
2 a memory storing a first identification key and a first transaction key;
3 and
4 a central processing unit coupled to the memory and configured to send
5 the first identification key and first transaction key to the smart card enabler,
6 and wherein the first enable signal and the second enable signal are received
7 from the smart card enabler based on the first identification key and first
8 transaction key.

1 10. The smart card of claim 9, wherein the memory also stores a first
2 transaction value, the first transaction value representing an available amount
3 of hard currency in electronic form for the smart card, and wherein the central
4 processing unit is also configured to send the first transaction value to the smart

5 card enabler such that the first transaction value is stored in the smart card
6 enabler.

1 11. The smart card of claim 10, wherein the central processing unit is also
2 configured to generate a second transaction value as a result of a transaction
3 and replace the first transaction value with the second transaction value.

1 12. The smart card of claim 11, wherein the central processing unit is also
2 configured to generate a second transaction key to replace the first transaction
3 key and transmit the second transaction key and second transaction value to
4 the smart card enabler.

1 13. A smart card enabler comprising:
2 first circuitry configured to receive a first identification key from a smart
3 card; and
4 second circuitry coupled with the first circuitry and configured to enable
5 the smart card to function with a smart card reader based on the first
6 identification key.

1 14. The smart card enabler of claim 13, wherein the first circuitry is also
2 configured to transmit a first enable signal to the smart card in order for the
3 smart card to function with the smart card reader, and wherein the second
4 circuitry is also configured to generate the first enable signal based on the first
5 identification key.

1 21. The smart card enabler of claim 17, wherein the second circuitry
2 includes:

3 a memory storing information received from the smart card.

1 22. The smart card enabler of claim 21, wherein the information stored in the
2 memory is also stored in the smart card.

23. The smart card enabler of claim 22, wherein the information includes transaction information comprising a transaction value representing an available amount of hard currency in electronic form used by the smart card.

1 24. The smart card enabler of claim 23, wherein the memory also stores a
2 second identification key and a second transaction key.

25. The smart card enabler of claim 24, further comprising:
a central processing unit configured to compare the first identification key from the smart card with the second identification key stored in the memory and compare the first transaction key from the smart card with the second transaction key stored in the memory to generate the first enable signal and the second enable signal, respectively, to the smart card.

1 26. A method for obtaining information stored in a smart card, the method
2 comprising:
3 recovering from the smart card information if the information is
4 incapable of being retrieved from the smart card using stored information in a
5 smart card enabler.

1 27. The method of claim 26, wherein the smart card is lost, damaged, or
2 destroyed.

1 28. The method of claim 26, wherein the information includes a transaction
2 value representing an available amount of hard currency in electronic form for
3 the smart card.

1 29. A method for using a smart card, the method comprising:
2 receiving a first identification key by a smart card enabler from the smart
3 card;
4 comparing the first identification key with a second identification key by
5 the smart card enabler; and
6 if the comparison of the first identification key with the second
7 identification key indicates the first identification key matches the second
8 identification key,
9 enabling the smart card to function with a smart card reader by the
10 smart card enabler.

1 30. The method of claim 29, wherein the first identification key and the
2 second identification key are fixed numbers.

1 31. The method of claim 29 further comprising:
2 receiving a first transaction key by the smart card enabler from the smart
3 card;
4 comparing the first transaction key with a second transaction key by the
5 smart card enabler; and

6 if the comparison of the first transaction key with the second transaction
7 key indicates the first transaction key matches the second transaction key,
8 enabling the smart card to perform a transaction with the smart card
9 reader by the smart card enabler.

1 32. The method of claim 31, wherein the first transaction key and the second
2 transaction key are randomly generated numbers.

1 33. The method of claim 31 further comprising:
2 performing a transaction by the smart card with the smart card reader
3 after being enabled to perform the transaction by the smart card enabler.

1 34. The method of claim 33 further comprising:
2 generating a third transaction key after performing the transaction
3 between the smart card and the smart card reader; and
4 replacing the first and second transaction keys with the third transaction
5 key.

1 35. The method of claim 34 further comprising:
2 creating a transaction value after performing the transaction between the
3 smart card and the smart card reader by the smart card, the transaction value
4 representing an available amount of hard currency represented in electronic
5 form as a result of the performed transaction; and
6 storing the transaction value in the smart card and smart card enabler.

1 36. The method of claim 35 further comprising:

2 recovering the transaction value from the smart card if the last
3 transaction value is incapable of being retrieved from the smart card using the
4 stored transaction value in the smart card enabler.

1 37. The method of claim 29, wherein receiving a first identification key
2 includes sending the first identification key by the smart card to the smart card
3 enabler periodically.

1 38. The method of claim 29, wherein the smart card enabler is within a close
2 proximity of the smart card and enables the smart card to function with the
3 smart card reader remotely using radio signals.

1 39. The method of claim 29, wherein if the comparison of the first
2 identification key with the second identification key indicates the first
3 identification key does not match the second identification key, the smart card
4 is disabled to function with the smart card reader.

1 40. The method of claim 31, wherein if the comparison of the first
2 transaction key with the second transaction key indicates the first transaction
3 key does not match the second transaction key, the smart card is disabled to
4 perform a transaction with the smart card reader.

1 41. The method of claim 34, wherein if the transaction is not performed
2 within a predetermined time period the smart card is disabled in performing
3 the transaction with the smart card reader.

1 46. The system of claim 42, wherein the smart card is also configured to
2 exchange transaction information with the smart card reader after being
3 enabled to perform a transaction, the transaction information including a first
4 transaction value representing an available amount of hard currency in
5 electronic form for the smart card.

1 47. The system of claim 44, wherein the smart card is also configured to
2 generate a third transaction key and transmit the third transaction key to the
3 smart card enabler.

1 48. The system of claim 47, wherein the smart card enabler is also configured
2 to replace the second transaction key with the third transaction key.

1 49. The system of claim 48, wherein the smart card is also configured to
2 generate a second transaction value representing an available amount of hard
3 currency in electronic form for the smart card as a result of the transaction with
4 the smart card reader, replace the first transaction value with the second
5 transaction value, and transmit the second transaction value to the smart card
6 enabler.

1 50. The system of claim 49, wherein the smart card enabler is also configured
2 to replace the first transaction value with the second transaction value, the first
3 transaction value and second transaction being stored in the smart card enabler.

1 51. The system of claim 50, wherein if the smart card is lost, damaged, or
2 destroyed the second transaction value from the smart card is recovered using
3 the second transaction value in the smart card enabler.

1 52. The system of claim 42, wherein the smart card is also configured to send
2 the first identification key to the smart card enabler periodically.

1 53. The system of claim 42, wherein the smart card enabler is also configured
2 to disable the smart card to function with the smart card reader if the
3 comparison of the first identification key with the second identification key
4 indicates the first identification key does not match the second identification
5 key.

1 54. The system of claim 44, wherein the smart card enabler is also configured
2 to disable the smart card to perform a transaction with the smart card reader if
3 the comparison of the first transaction key with the second transaction key
4 indicates the first transaction key does not match the second transaction key.

1 55. The system of claim 42, wherein the smart card and smart card enabler
2 are configured to communicate with each other using radio signals.

1 56. The system of claim 42, wherein the smart card and smart card reader
2 are configured to communicate with each other using radio signals.

1 57. The system of claim 42, wherein the smart card enabler enables the smart
2 card within a close proximity of the smart card.

1 58. The system of claim 42, wherein the smart card enabler is configured to
2 attach with the smart card, and wherein the smart card and the smart card
3 enabler operate as a single unit.

1 59. The system of claim 42, wherein the smart card is configured such that if
2 it is not enabled to function with the smart card reader after a predetermined
3 time period the smart card is disabled to operate.

add
A2